PRL

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/878,468	06/11/2001	Santanu Dutta	12604- US1 (011317-021)	2673

24239 7590 11/04/2004

MOORE & VAN ALLEN, PLLC
2200 W MAIN STREET
SUITE 800
DURHAM, NC 27705

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/878,468	DUTTA ET AL.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *04 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/20/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-51 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meche et al. , US patent 5600708, in view of Kravitz, US patent 5231668, in further view of Gustafsson, US patent 6424841.

In reference to claim 1:

Meche et al. (Column 5, lines 45-61) discloses a method of remotely controlling a security element of a mobile terminal for disabling and enabling access to secured functions of the mobile terminal, the method comprising:

- Receiving a request from a user, where the user is the MT or Mobile Terminal, and the request is an authentication request received by the MSC. (Figure 1, MT)
- Verifying authenticity of the user, where the MSC proceeds to verify the authenticity of the user through an identity request and identity response check. (Column 4, lines 21-32)

- Creating a push message which causes a disablement application to be executed. (Column 6, lines 8-18)
- Sending the push message to the mobile terminal, where the push message is RAND. (Column 6, lines 8-18)

Meche et al. however fails to explicitly disclose a method wherein the push message for the mobile terminal is signed.
Kravitz discloses a digital signature algorithm. Kravtiz (Column 1, lines 10-20) discloses that a digital signature may be used for security when the receiving party of the message wants to be sure of the identity of the sender party.

Meche et al. fails to explicitly disclose a method where the push message includes an address. Gustafsson discloses a method of transmission between mobile units where an address is included with the message. Addresses provide the advantage of knowing where to send a message.

It would have been obvious to one of ordinary skill in the art to sign the disabling push message for the application in order to prevent the reception of fraudulent disablement messages and to include an address in the transmission in order to specify where the disablement message is to be sent to.

In reference to claim 2:

Meche et al. discloses the method of claim 1 wherein the request and the push message are for disabling access, and further comprising:

- Receiving a confirmation message from the mobile terminal, where the confirmation message is the yes or no to determine if the lock is on. (Figure 2, Item 320)
- Sending a response message to the user based on the confirmation message, where a response is sent by sending a security request to turn the IMEI lock on. (Figure 2, Item 325)

In reference to claim 3:

Meche et al. (Column 6, lines 9-18) discloses the method of claim 1 wherein the request from the user and the push message are for disabling access, and further comprising:

- Determining that the mobile terminal is unavailable, where the mobile terminal is unavailable for future use if it is determined to be stolen and blacklisted. (Column 3, lines 15-22)
- Sending a response message to the user based on a determination that the mobile terminal is unavailable, where the response message that is sent to the user of the MT is a disabling request. (Column 6, lines 9-18)

In reference to claim 4:

Meche et al. fails to discloses the method of claim 2 wherein the confirmation message (Column 6, lines 32-36) from the mobile terminal is signed.

Kravitz discloses a digital signature algorithm. Kravtiz (Column 1, lines 10-20) discloses that a digital signature may be used for security when the receiving party of the message wants to be sure of the identity of the sender party.

It would have been obvious to one of ordinary skill in the art to sign the confirmation message to in order to prevent the reception of fraudulent disablement messages and allow for the authentication of the confirmation message.

In reference to claim 5:

Meche et al. fails to explicitly disclose the method of claim 4 wherein the combination message and the response include position information for the mobile terminal.

Meche et al. (Column 4, lines 34-52) however discloses this in a previous confirmation message, where the information of the transmissions is packaged into a location updating request.

It would have been obvious to one of ordinary skill in the art to perform the location updating request in a response for the mobile terminal, in order to gather the MT's current location if the MT is responsive.

Claim 6 substantially similar to claim 2 and is rejected for the same reasons.

In reference to claim 7:

Meche et al. (Figure 1, Item 10) discloses the method of claim 1 wherein the content comprises an identification of an application that resides in the mobile terminal, where the application that resides on the mobile terminal is identified by the IMEI. (Column 3, lines 50-57)

In reference to claim 8:

Meche et al. (Column 6, lines 8-18) discloses the method of claim 1 wherein the content comprises an identification of a calling program residing at a server, where the identification of the calling program residing at the server is the authentication of the SRES sent out by the calling program to disable the MT.

9, 11, 13, 15, 17, 21, 27 is rejected for the same reasons as claim 7.

10, 12, 14, 16, 18, 22, 28 is rejected for the same reasons as claim 8.

Claim 19, 20 is rejected for the same reasons as claim 2.

In reference to claim 23:

Meche et al. discloses the computer program product of claim 20 further comprising:

- Instructions for receiving information for the mobile terminal within a signed confirmation message from the mobile terminal when the request and the push message are for disabling access, where the push message disables access (Column 6, lines 8-18)

- Instructions for including the position information for the mobile terminal in the response, where the position information is included in the location updating request. (Column 4, lines 34-52)

Meche et al. fails to explicitly disclose a signed push message and the inclusion of position information in the conformation message.

As noted in claim 1, it would have been obvious to one of ordinary skill in the art to sign the disabling push message in order to authenticate the sender of the message to disable access so that not just anyone would be able to remotely disable the functions of the phone.

Claims 24, 25, 29, 30, 31 are rejected for the same reasons as claim 23.
Claim 26 is rejected for the same reasons as claim 2.

In reference to claim 32:
Meche et al. discloses a system for controlling a security element of a mobile terminal for disabling and enabling access to secured functions of the mobile terminal, the system comprising:

- A push initiator operable to create and send signed push messages including, at least, an address for the mobile terminal and content which causes a disablement application to be executed. (Column 6, lines 8-18)

- A proxy gateway operable to receive the signed push message and send over-the-air messages to the mobile terminal corresponding to the push messages, where the message is sent over-the-air to the MT (Column 6, lines 8-18)
- A network interconnecting the push initiator and the proxy gateway, where the network is shown to be figure 1. (Figure 1)

Meche et al. fails to explicitly disclose an embodiment wherein the push message is signed.

Kravitz discloses a digital signature algorithm. Kravtiz (Column 1, lines 10-20) discloses that a digital signature may be used for security when the receiving party of the message wants to be sure of the identity of the sender party.

It would have been obvious to one of ordinary skill in the art to sign the push message to disable the application in order to prevent the reception of fraudulent disablement messages and allow for the authentication of the push message.

In reference to claim 33:

Meche et al. (Figure 1, Item 10) discloses a mobile terminal comprising:

- A radio block (Figure 1, Item 10)
- A security element encoded with at least one security key for securing transactions, where the security element is the application within the MT, and the security key is the IMEI. (Figure 1, Items 15 & 20)

- A processor system operably connected to the radio block and the security element, the processor system further operable to disable and enable access to the key in response to the unsolicited, over-the-air messages received through the radio block, where the processor is the microcontroller. (Figure 1, Item 10)

In reference to claim 34:

Meche et al. fails to explicitly discloses the mobile terminal of claim 33 wherein the processor system is further operable to disable access to the at least one security key while permitting operations of the security element for which user authentication and authorization services are not required.

It would have been obvious to one of ordinary skill in the art to continue to allow functions that didn't require authorization services to continue to function such as power on/off or the number pad to a mobile terminal.

In reference to claim 35:

Meche et al. discloses the mobile terminal of claim 33 wherein the processor system disables access to the at least one security key by disabling access to the security element, where the security key that is disabled is the IMEI. (Column 6, lines 8-18)

In reference to claim 36:

Meche et al. discloses the mobile terminal of claim 34 wherein the security element further comprises at least one status register associated with the at least one security key (Column 3 lines

15-22), and wherein the processor system enables and disables access to the key by alternatively setting the status register to a first state wherein access to the at least one security key is enabled and a second state wherein access to the at least one security key is disabled, respectively(Figure 2, Items 320 and 325),

where the status register is the list which determines should the MT be made accessible or not on the stolen list where the security key associated is the IMEI and UIM

In reference to claim 37:

Meche et al. fails to discloses the mobile terminal of claim 33 further comprising a global positioning system (GPS) subsystem, where the position information being retrieved from the GPS subsystem.

Meche et al. discloses.

and wherein the processor system is further enabled to cause the mobile terminal to send a confirmation message through the radio block, the confirmation message including position information for the mobile terminal,

The Examiner takes official notice that retrieving a position using a GPS subsystem was well known in the art at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to retrieving a position using a GPS because of the flexibility it provides in being able to locate an object.

Claims 38, 39, 50, 51 is rejected for the same reasons as claim 37.

In reference to claim 40:

Meche et al. (Figure 2, Items 320 and 325), discloses a security element for a mobile terminal, the security element encoded with a data structure for providing user authentication services, the data structure comprising:

- At least one key for securing at least some transactions initiated by a user of the mobile terminal, where the key is the IMEI and UIM. (Column 3, lines 15-22)
- At least one status indicator associated with the at least one key, the status indicator settable by the mobile terminal alternatively to a first state wherein access to the at least one key is enabled and a second state wherein access to the at least one key is disabled, where the status indicator indicates whether the MT has been IMEI locked or not. (Figure 2, Items 320 and 325),

In reference to claim 41:

Meche et al. discloses the security element of claim 40 wherein the at least one key is a plurality of key pairs providing user authentication and authorization services through the use of digital signatures, and wherein the at least one status indicator is a plurality of status indicators, further wherein each status indicator is associated with one key pair.

Meche et al. fails to explicitly disclose the use of digital signatures and the associated key pairs inherent to the use thereof.

Kravitz discloses a digital signature algorithm. Kravtiz (Column 1, lines 10-20) discloses that a digital signature may be used for security when the receiving party of the message wants to be sure of the identity of the sender party.

Inherent to the function of a digital signature is the use of a key pair in which a private key is used to digitally sign or encrypt a document, while the public key is used to decrypt or verify the signature. (Column 4, lines 59-63)

It would have been obvious to one of ordinary skill in the art at the time of invention to use a key pair to provide authentication and authorization services through the use of a digital signature for the advantage that it's a well understood, and easily implementable method of authentication in the cryptographic arts.

In reference to claim 42:

Meche et al. discloses:

In a mobile terminal, a method of controlling access to a security key in a security element, the method comprising:

- Receiving an unsolicited, over-the-air request to disable access to the security key in the security element, (Column 6, lines 9-18)

- Updating a status register in the security element to disable access to the security key (Figure 3, Items 110, 145)
- Sending an over the air secured confirmation message indicating success of disabling access to the security key. (Column 6, lines 9-18) & (Figure 3, Item 146)

In reference to claim 43:

Meche et al. fails to disclose the method of claim 42 further comprising:

- Receiving an unsolicited, over the air request to re-enable access to the security key in the security element.
- Updating a status register in the security element to re-enable access to the security key.

Meche et al. discloses a method of operation comprising the sending of message over the air in order to disable access to the security key in the security element.

The Examiner takes official notice that the concept of re-enabling a disabled application, or unlocking a locked item was well known in the art at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to re-enable access to the security key in the security element, and update the status registers associated with it in order to allow access to a mobile unit once it is determined that access should be given.

In reference to claim 44:

Meche et al. fails to explicitly discloses the method of claim 42 wherein the unsolicited over the air request to disable access takes the form of a wireless application protocol (WAP) push message.

The Examiner takes official notice that WAP, the wireless application protocol was well known in the art as a means of encoding the transmissions between wireless devices. Its use was and is still prevalent among mobile terminals.

It would have been obvious to one of ordinary skill in the art at the time of invention to encode the transmissions to the MT using WAP in order to transmit the information in a protocol commonly used by other vendors and companies, and well understood by others at the time.

Claim 45 is rejected for the same reasons as claim 44.

Claim 46 is rejected for the same reasons as claim 42.

Claim 47 is rejected for the same reasons as claim 33.

Claim 48 is rejected for the same reasons as claim 34.

Claim 49 is rejected for the same reasons as claim 35.

Conclusion

4. The following art not relied upon is made of record:

Rohrbach, US patent 5,898,783 discloses a method to remotely disable a smart or sim card in a mobile unit.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

October 28th, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100